Cryptography, Moore's Law, and Hardware Foundations for Security

Paul Kocher
Cryptography Research Division, Rambus

Keynote Session
ICMC 2015
November 5, 2015

Rambus
CRYPTOGRAPHY RESEARCH

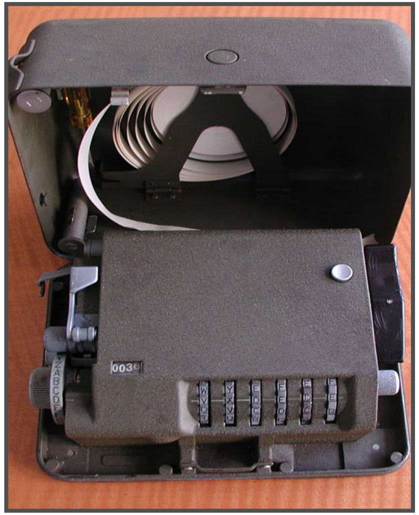
The information contained in this presentation is provided for educational purposes only, and is provided without any guarantee or warranty whatsoever, and does not necessarily represent official opinions of Cryptography Research, Rambus, or their partners.

Background

- Started Cryptography Research 1995
  - Business model evolved (Consulting + R&D → IP licensing → solutions)
  - Organic growth, no outside investors thru acquisition by Rambus in 2011 ($342.5M)

- Selected projects:
  - **SSL v3.0 / TLS:** Co-authored security protocol
  - **Timing attacks; Differential power analysis:** Side channel attacks & countermeasures
  - **Deep Crack:** Hardware with a custom SoC to break DES
  - **ValiCert:** Co-founded start-up (IPO in 2001, acquired 2003)
  - **CryptoFirewall Cores:** Tamper-resistant cores to stop video piracy & counterfeiting
  - **BD+:** Renewable security solution in Blu-ray
  - **Vidity (SCSA):** Security for a new video distribution format (just launched)
  - **Cryptography Research Fund for Students:** $1M fund w/ IACR to support students
  - **CryptoManager:** Leading ASIC security solution (incl. on-chip cores, infrastructure)

Changing Device Security Constraints

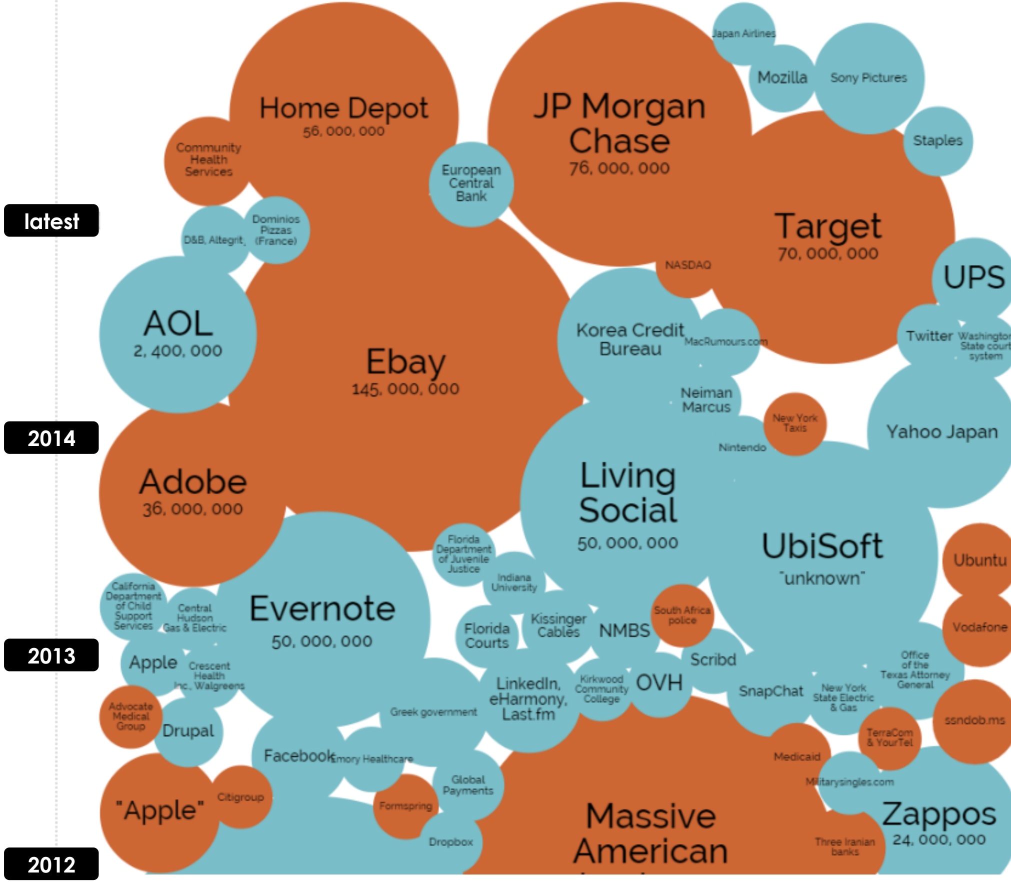


- Security used to be limited by computing power
- More computing power enables much stronger algorithms
  - Example of 3DES: 3X computation = 2^{56}X strength vs. brute force

… but Something is Very Wrong

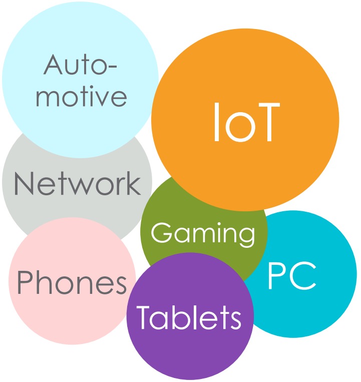
- Increasing breaches at all levels
- Within two years, 90% of all IT networks will have an IoT-based security breach (source: IDC)
- What happens if we have 50B connected devices by 2020?

Sources: DataBreaches.net, IdTheftCentre



Computing & Security Trends

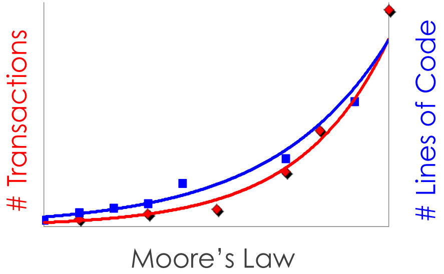
More Devices


Auto-motive
IoT
Network
Gaming
PC
Phones
Tablets

More Valuable Data

ID
cloud
passwords
Breaches
payments
DRM
IP

More Complexity

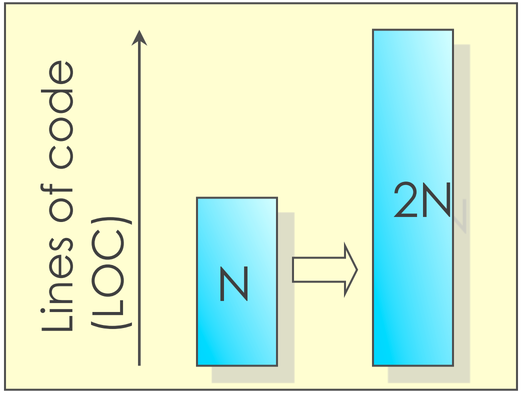


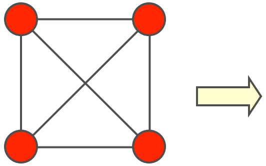
More Targets

More Attacker Reward

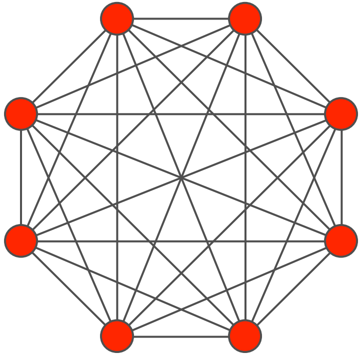
More Vulnerabilities

What Emerges as Complexity Increases?





**4 elements:
6 interactions**



**8 elements:
28 interactions**

- If defect density is constant per element, odds of zero flaws squares (20% → 4%)

- Reality is worse:
  - Defects reflect interactions (4th power)
  - Defect densities tend to increase

Silver Bridge on U.S. 35 in Ohio: Built 1924

Collapsed in 1967, created awareness of "fracture critical components"

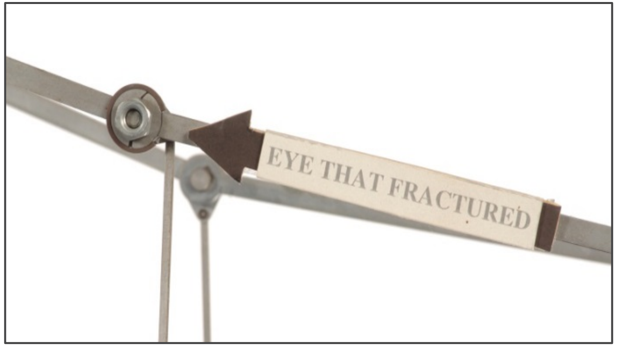


Image from model of bridge, courtesy of NIST

How many "fracture-critical" elements are in a typical IoT device?

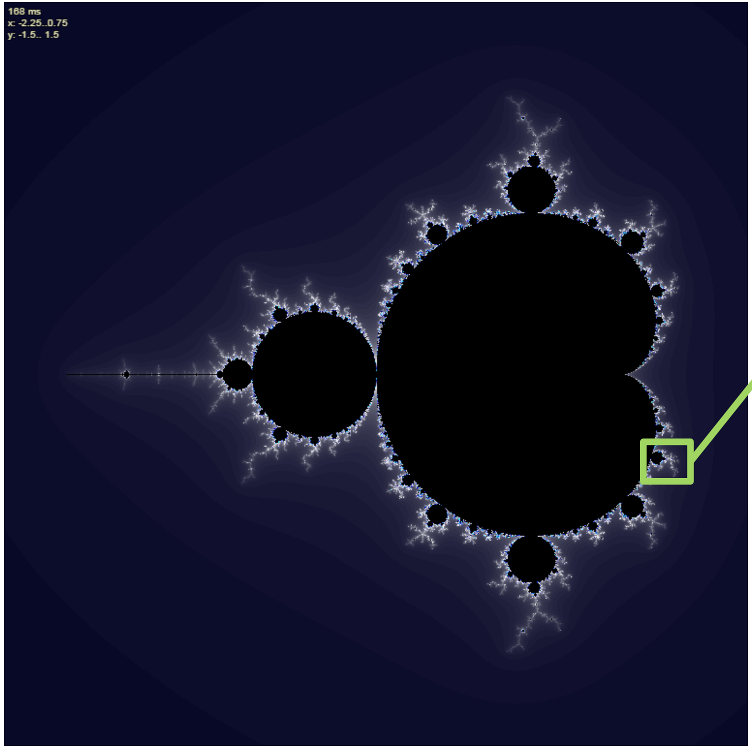
- Bits of DRAM (non-ECC)
- Bits of flash/storage
- CPU logic
- Support logic
- Software
- Infrastructure

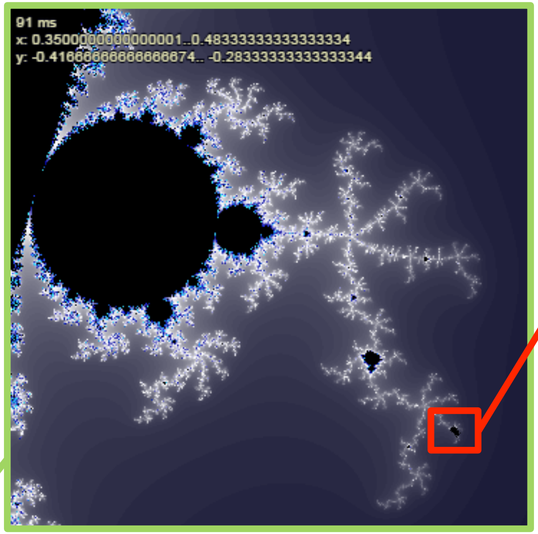
…

~10 billion (10^{10}) today…

In 10 years ~1 trillion (10^{12})

Security & Fractals




91 ms
x: 0.35000000000000001..0.48333333333333334
y: -0.41666666666666674.. -0.28333333333333344

31 ms
x: 0.46..0.46777777777777778
y: -0.39703703703703713.. -0.38925925925925936

```
    goto fail;
 r ((err = SSLHash
    goto fail;
if ((err = SSLHashSH
    goto fail;
    goto fail;
if ((err = SSLHashSHA
    goto fail;

    err = sslRawV
```

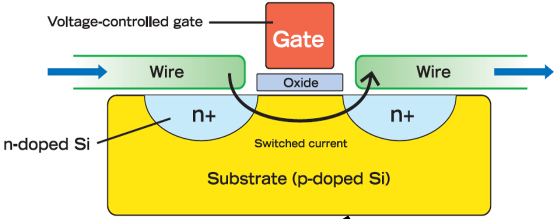
Individual bugs are "obvious"
– when we stare directly at them

Overall risks are "obvious" too
– if we look for them

- Our ability to understand simple elements often creates a **false impression** that we understand the complex system

Insecurity is an emergent property.

Transistor



Machine Language

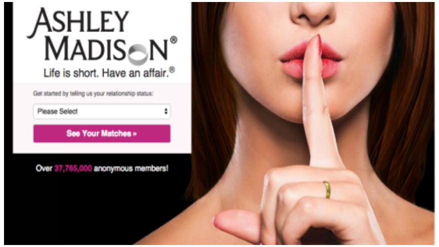
```
00401880   push    ebp
00401881   mov     ebp,esp
00401889   push    0
0040188B   call    004019b0
00401890   add     esp,4
00401893   jmp     004018d1
00401898   push    eax
00401899   call    004018e0
0040189E   add     esp,4
```

Network

Processor,SoC

Operating System

"Secure" Services



ASHLEY MADISON®

Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select

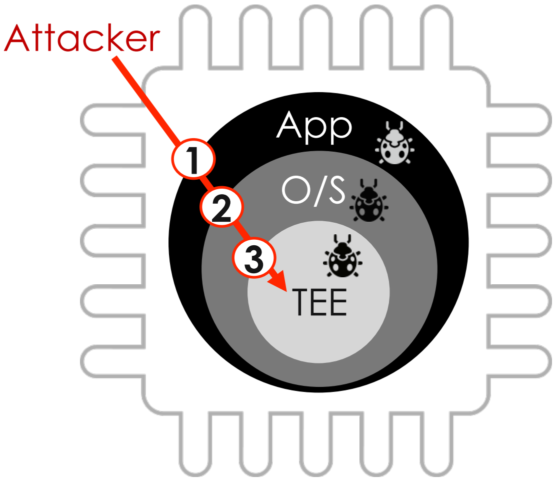
See Your Matches »

Over 37,765,000 anonymous members!

Incorrect Assumptions: Two SoC Examples

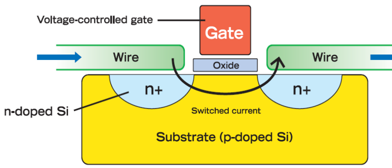
Defect Densities

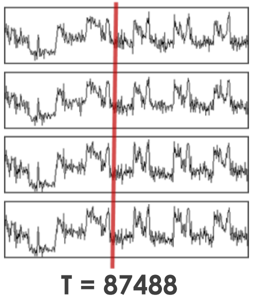
- **Assumption:** Software will be bug-free
- **Reality:** Current designs are 1-3 exploits from total breach, with overwhelming likelihood of vulnerabilities

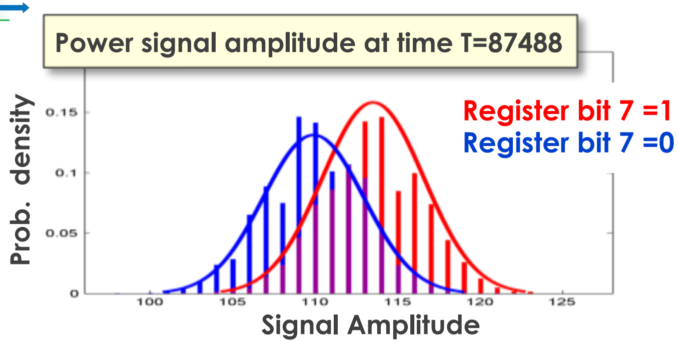


Side Channels

- **Assumption:** Attackers only see the binary input/output data
- **Reality:** Power & RF measurements show tiny correlations to individual gates -- that compromise keys from large, busy SoCs







~9B chips/year made with countermeasures we license

Four Properties for Solutions to Succeed

Hardware-based

Hardware is the only layer where we know how to build reliable security boundaries

Deployable additively

Legacy designs can’t be abandoned, but are too complex to retrofit

Addresses infrastructure

Solutions that must address both in-device capabilities and manufacturing/lifecycle

Broadly positive ROI

All stakeholders must benefit, and benefits must not depend on ubiquity

Perimeters

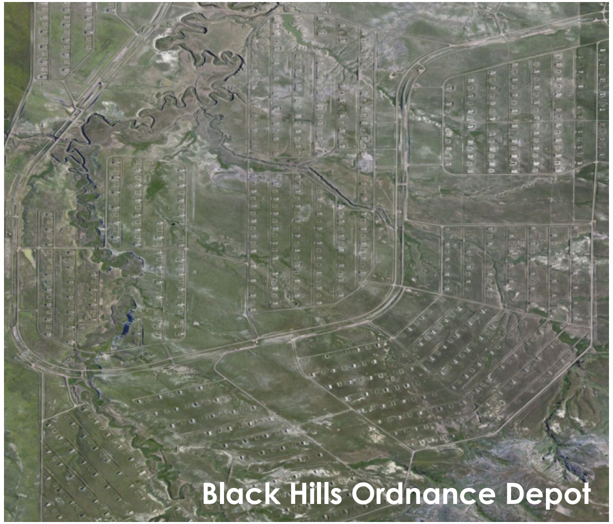
Grow in a single security perimeter

Serbian ammunition storage facility

Traditional approach for security enhancements in CPUs, OSes…

Failure is likely + catastrophic

Add additional partitions



Black Hills Ordnance Depot

Many small security perimeters, e.g. for each use case

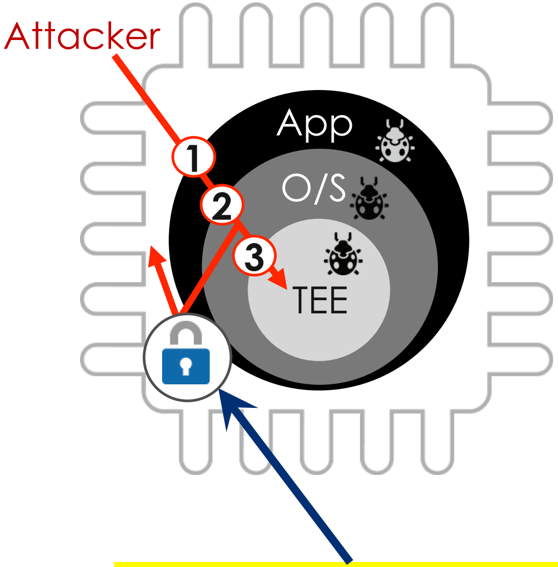
Small, survivable failures

Solving the problem

- Software security is not scalable
  - No hope of eliminating bugs in existing software
  - Macro situation is getting worse, not better
  - CPU modes (TrustZone, Ring 0) haven't helped despite decades of trying

- Separate chips/modules only work for a small subset of use cases (but can be great)
  - Costly; distant from where security is needed

- Secure 'on-SoC' logic blocks
  - On the SoC with intra-chip security perimeter
  - Isolated from main CPUs, SoC fabric, DRAM, …



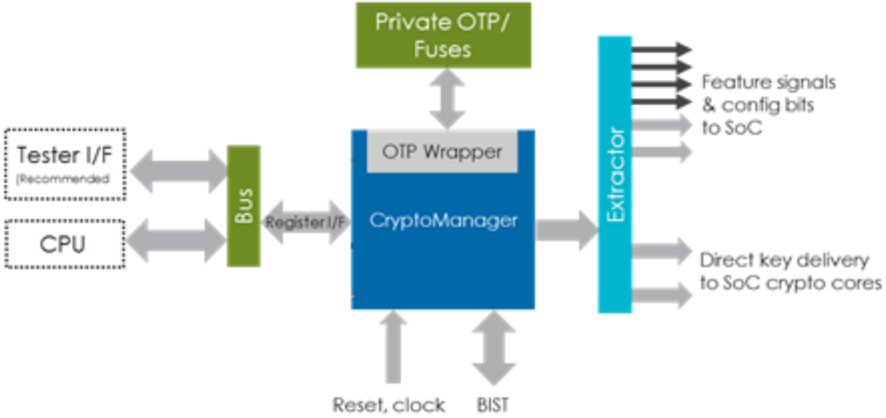
On-SoC secure HW

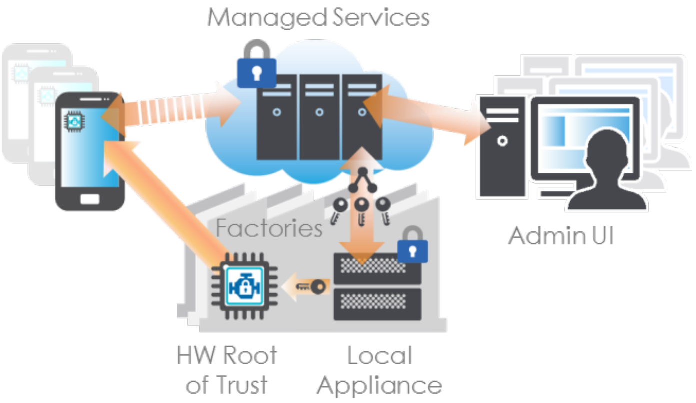
On-Die Security Modules

- Why are on-chip security solutions particularly important?
  - Integration enables major security advantages
  - 10X-100X cheaper to manufacture
  - = Far greater potential reach than separate chips/modules (despite complex economics of certification)
- Challenges are solvable, e.g.:
  - Analog countermeasures → digital countermeasures
  - NVM → OTP
  - Appliance-to-core secure tunnels & multi-stage perso allow factories to be untrusted
  - Third-party IP vendors can address chipmakers' lack of security expertise
- Harnessing Moore's Law
  - Moore's Law **helps** security: On-die transistor prices fall
    - Separate modules don't benefit due to non-transistor costs (packaging, distribution…)
  - Potential for many security modules per chip (like CPU proliferation)
    - Specialization for payments, VPN, content protection, identification…

Cryptography Research Approach: CryptoManager Solution

Observation: Chipmakers required solutions for in-device security **and** also solutions for enabling infrastructure



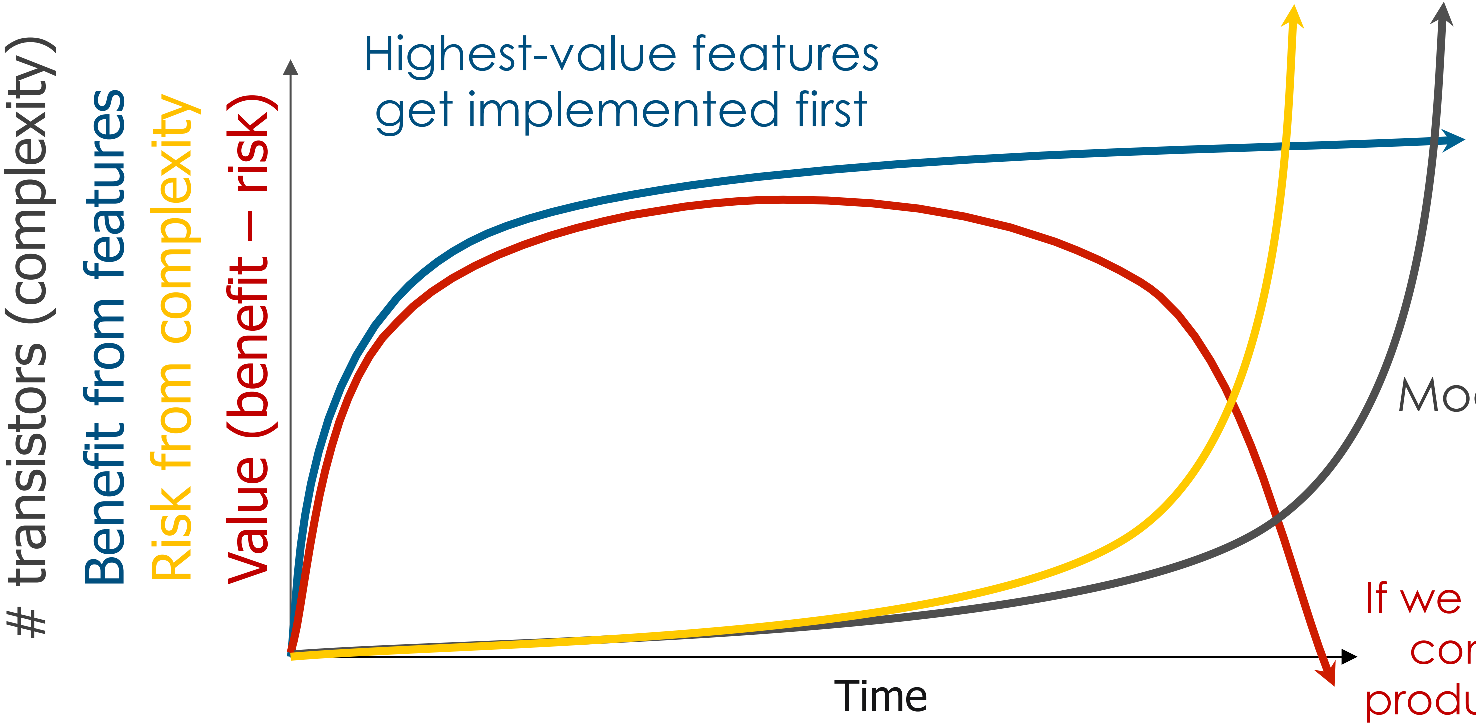


CryptoManager Core protects keys, configuration, debug settings, etc. throughout SoC

CryptoManager Infrastructure delivers and audits security transactions across factories & data centers

Looking Ahead…

Security Risks Limit Technology's Value



Risk grows with complexity

Highest-value features get implemented first

Moore's Law

If we can't control risk, complexity makes products ***less valuable***

"Russian guard service reverts to typewriters after NSA leaks" -- The Guardian (July 11, 2013)

"Indian High Commission in London to use Typewriters following Snowden Expose" -- Authint Mail (Oct. 25, 2013)

Looking Ahead

- “May you live in interesting times …”
  - Macro trend of worsening will continue for 3-5 years *minimum*
  - Individual designs may fare much better/worse
- Technology industry’s future depends on finding solutions
  - Otherwise, security risks will erase net benefits from new technology

+

1995 Mercedes

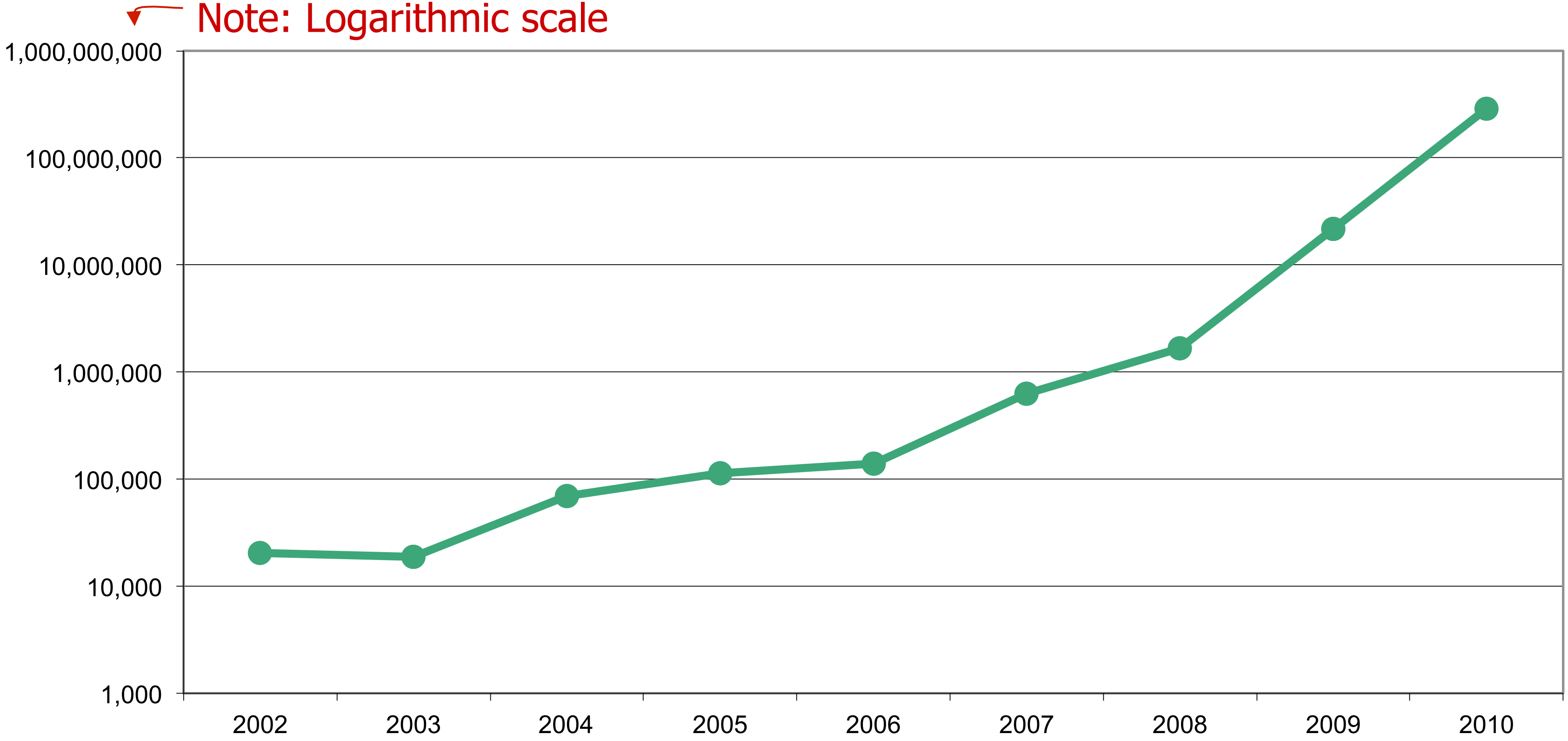
  - Past analogies: safety (aviation, pharma), environment (manufacturing)
- Security modules will play a leading role in managing risk

Thank You

Rambus CRYPTOGRAPHY RESEARCH

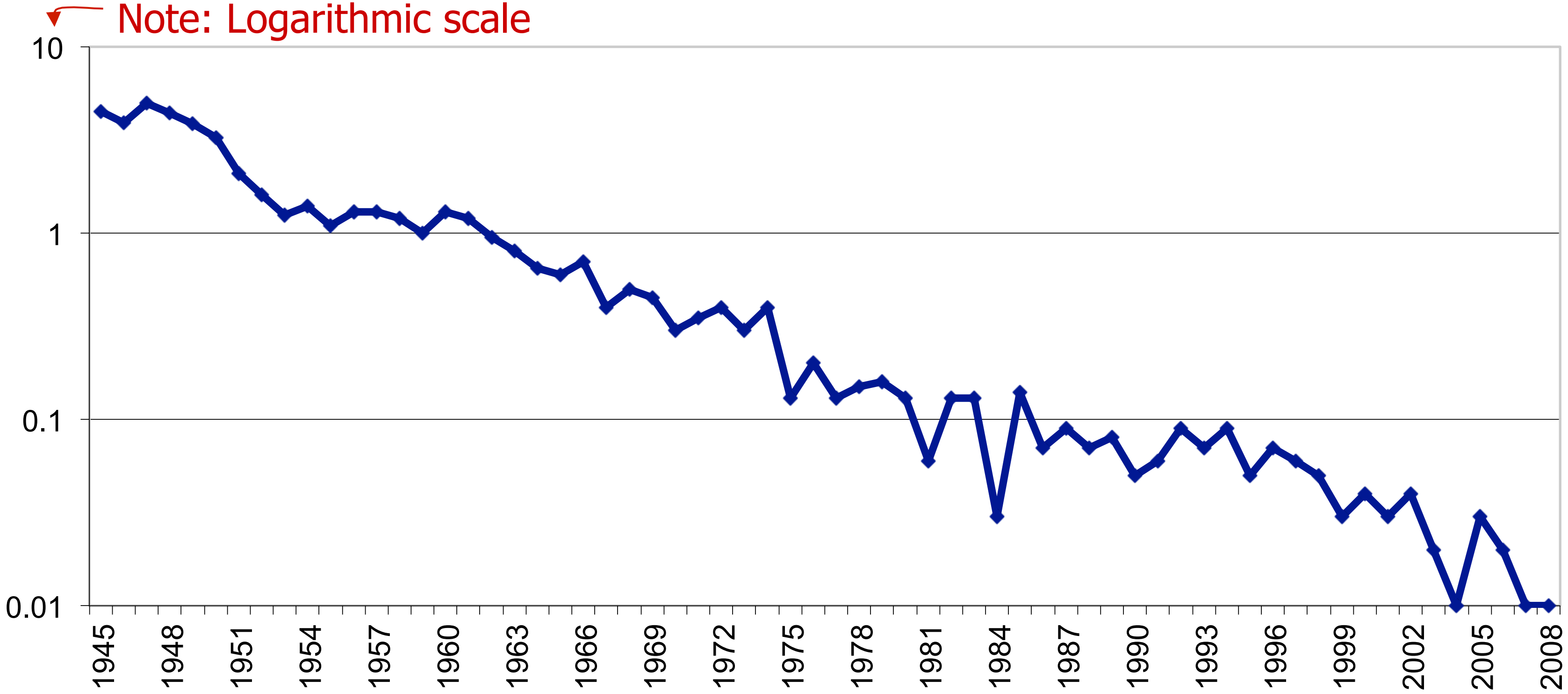
Number of New Threats Each Year
(per data from Symantec)

Note: Logarithmic scale



Fatalities per 100M Passenger Miles

(For scheduled service; excludes "unlawful interference" and USSR)


Note: Logarithmic scale